BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

JP11032037
CERTIFICATION DATA GENERATING DEVICE

FUJI XEROX CO LTD
Inventor(s): ;NAKAGAKI JUHEI ;SHIN YOSHIHIRO
Application No. 09188801 , **Filed** 19970714 , **Published** 19990202

Abstract:

PROBLEM TO BE SOLVED: To pre-pay access qualification to purchase or rent without imposing any surplus load on a certification data generating device side.

SOLUTION: A pre-paid purchase ticket $T_2$is stored in an access ticket storing part 13. Next, (T_1', n_2) is inputted to a certification data-imputting part 14. A use condition judging part 15 extracts a corresponding access ticket (t_2, L_2, n_2), checks whether or not a use condition $L_2$is fulfilled, and reduces frequency information V, when the use condition is fulfilled. A certification data generating and outputting part 16 calculates certification data R by using auxiliary certification decision $(t)_2$and the use condition L_2 extracted by the use condition decision part 15 and (du) read from a user specific information storing part 11, and outputs T_1. A user performs access to a program in a purchase state or a rent state by using the T_1.

Int'l Class: H04L00932 G06F00906 G06F01500 G09C00100

MicroPat nt Reference Number: 000373409

PatentWeb Home | Edit Search | Return to Patent List | Help

For further information, please contact:
Technical Support | Billing | Sales | General Information

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－32037

(43)公開日　平成11年(1999)２月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	15/00	３３０		15/00	３３０Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
					６４０Ｅ

審査請求　未請求　請求項の数11　ＯＬ　（全 18 頁）

(21)出願番号　特願平9－188801

(22)出願日　平成９年(1997)７月14日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　申　吉浩
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

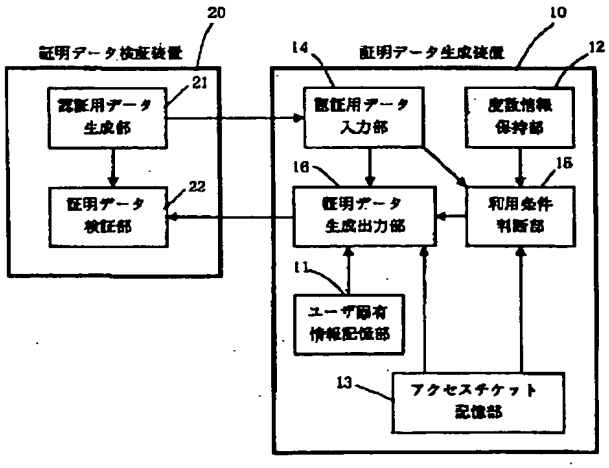
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　証明データ生成装置

(57)【要約】

【課題】　証明データ生成装置側に余分な負荷をかけることなく、買い取りやレントのアクセス資格をプリペイドで支払う。

【解決手段】　プリペイド払いパーチェス・チケットのT_2はアクセスチケット記憶部１３に格納される。次に、（T_1'，n_2）が認証用データ入力部１４に入力される。利用条件判断部１５は、対応するアクセスチケット（t_2，L_2，n_2）を取り出し、利用条件L_2が満たされるか調べ、満たされれば、度数情報Ｖを減額する。証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報t_2、利用条件L_2と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算してT_1を出力する。ユーザはT_1を用いて買い取り状態であるいはレント状態でプログラムへのアクセスを行う。



実施例の構成図

【特許請求の範囲】

【請求項１】　ユーザのアクセス資格を認証するために生成され、正当性を検証される証明データを生成する証明データ生成装置において、

認証用データを入力する認証用データ入力手段と、

ユーザの固有情報を記憶するユーザ固有情報記憶手段と、

ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した利用条件情報とに対し、所定の計算を実行して生成した証明用補助情報と、利用条件情報との組を含む証明用補助情報セットを記憶する証明用補助情報セット記憶手段と、

入力された認証用データに対応する証明用補助情報セットを上記証明用補助情報セット記憶手段から取り出し、上記取り出した証明用補助情報セットの利用条件情報に従い、以降の処理を継続するかどうかの判断を行う利用条件判断手段と上記利用条件判断手段において継続と判断されたときに、上記取り出した証明用補助情報セットと、上記認証用データ入力手段から入力された認証用データと、上記ユーザ固有情報記憶手段に記憶されている上記ユーザの固有情報とに所定の計算を施して証明データを生成し出力する証明データ生成出力手段とを有し、

上記認証用データ入力手段から、第１の証明用補助情報セットを暗号関数における暗号化鍵で暗号化した暗号化証明用補助情報セットを入力し、

上記利用条件判断手段は、上記証明用補助情報セット記憶手段から、入力された暗号化証明用補助情報セットに対応する第２の証明用補助情報セットを取り出し、上記取り出した第２の証明用補助情報セットの利用条件情報に従い、所定の処理を行った後、以降の処理を継続するかどうかの判断を行い、

上記証明データ生成出力手段は、上記処理を行うことにより、上記暗号化証明用補助情報セットを復号化した結果である第１の証明用補助情報セットを出力することを特徴とする証明データ生成装置。

【請求項２】　少なくとも、上記ユーザ固有情報記憶手段と、上記利用条件判断手段と、上記証明データ生成出力手段とが、内部のデータおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保持されている請求項１記載の証明データ生成装置。

【請求項３】　さらに電子度数情報を保持する度数情報保持手段を備え、上記利用条件情報には、利用したときに支払うべき利用度数を含み、上記利用条件判断手段は、上記度数情報保持手段に保持されている電子度数情報と、上記利用条件情報に含まれる利用度数とを比較して、上記度数情報保持手段に保持されている電子度数情報が利用条件情報に含まれる利用度数以上の時にのみ、上記度数情報保持手段に保持されている電子度数情報から上記利用条件情報に含まれる利用度数分の度数を減額して、以降の処理を継続するという判断を行う請求項１または２記載の証明データ生成装置。

【請求項４】　上記第１の証明用補助情報セットに含まれる第１の利用条件情報に含まれる利用度数は０度数であり、上記第２の証明用補助情報セットに含まれる第２の利用条件情報に含まれる利用度数は０以外であることを特徴とする請求項３記載の証明データ生成装置。

【請求項５】　さらに時刻を示す時計を備え、上記第１の証明用補助情報セットに含まれる第１の利用条件情報には、さらに有効期限情報が記載され、上記利用条件判断手段は、上記時刻と上記有効期限情報とを比較し、該時刻が有効期限内にある時にのみ、以降の処理を継続するという判断を行う請求項１、２、３または４記載の証明データ生成装置。

【請求項６】　少なくとも、上記証明用補助情報セット記憶手段以外の手段が、携帯可能な小型演算装置として構成されている請求項１、２、３、４または５記載の証明データ生成装置。

【請求項７】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置において、

認証用データを記憶する第１の記憶手段と、

ユーザの固有情報を記憶する第２の記憶手段と、

上記ユーザの固有情報と、アクセス資格認証の特徴情報とに対して所定の計算を実行して生成した第１の証明用補助情報を暗号化して生成した暗号化証明用補助情報を記憶する第３の記憶手段と、

上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した利用条件情報とに対して、所定の計算を実行して生成した第２の証明用補助情報と、上記利用条件情報とからなる第２の証明用補助情報セットを記憶する第４の記憶手段と、

上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットに含まれる上記利用条件情報にしたがって所定の処理を継続するかどうかを判断する手段と、

上記所定の処理を継続すると判断したときに、上記第３の記憶手段に記憶されている上記暗号化証明用補助情報と、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットとに対して所定の計算を実行して上記第１の証明用補助情報を復元する手段と、

上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、復元した上記第１の認証用補助情報とに対して所定の計算を実行して証明データを生成する手段と、

生成された上記証明データを検証する手段とを有することを特徴とするアクセス資格認証装置。

【請求項８】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上

記ユーザのアクセス資格を認証するアクセス資格認証装置において、
認証用データを記憶する第１の記憶手段と、
ユーザの固有情報を記憶する第２の記憶手段と、
上記ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して生成した第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化して生成した暗号化証明用補助情報セットを記憶する第３の記憶手段と、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して生成した第２の証明用補助情報と、上記第２の利用条件情報とからなる第２の証明用補助情報セットを記憶する第４の記憶手段と、
上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットに含まれる上記第２の利用条件情報にしたがって第１の処理を継続するかどうかを判断する手段と、
上記第１の処理を継続すると判断したときに、上記第３の記憶手段に記憶されている上記暗号化証明用補助情報セットと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、上記第４の記憶手段に記憶されている上記第２の証明用補助情報セットとに対して所定の計算を実行して上記第１の証明用補助情報セットを復元する手段と、
復元された上記第１の証明用補助情報セットに含まれる上記第１の利用条件情報にしたがって第２の処理を継続するかどうかを判断する手段と、
上記第２の処理を継続すると判断したときに、上記第１の記憶手段に記憶されている上記認証用データと、上記第２の記憶手段に記憶されている上記ユーザの固有情報と、復元した上記第１の証明用補助情報セットとに対して所定の計算を実行して証明データを生成する手段と、
生成された上記証明データを検証する手段とを有することを特徴とするアクセス資格認証装置。
【請求項９】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証方法において、
認証用データを記憶する第１のステップと、
ユーザの固有情報を記憶する第２の記憶ステップと、
上記ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して生成した第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化して生成した暗号化証明用補助情報セットを記憶する第３のステップと、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して生成した第２の証明用補助情報と、上記第２の利用条件情報とからなる第２の証明用補助情報セットを記憶する第４の記憶ステップと、
上記第４の記憶ステップで記憶された上記第２の証明用補助情報セットに含まれる上記第２の利用条件情報にしたがって第１の処理を継続するかどうかを判断するステップと、
上記第１の処理を継続すると判断したときに、上記第３の記憶ステップで記憶された上記暗号化証明用補助情報セットと、上記第１の記憶ステップで記憶された上記ユーザの固有情報と、上記第４の記憶ステップで記憶された上記第２の証明用補助情報セットとに対して所定の計算を実行して上記第１の証明用補助情報セットを復元するステップと、
復元された上記第１の証明用補助情報セットに含まれる上記第１の利用条件情報にしたがって第２の処理を継続するかどうかを判断するステップと、
上記第２の処理を継続すると判断したときに、上記第１の記憶ステップで記憶された上記認証用データと、上記第２の記憶ステップで記憶された上記ユーザの固有情報と、復元した上記第１の証明用補助情報セットとに対して所定の計算を実行して証明データを生成するステップと、
生成された上記証明データを検証するステップとを有することを特徴とするアクセス資格認証方法。
【請求項１０】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に用いる証明用補助情報を生成する証明用補助情報生成装置において、
ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して第１の証明用補助情報を生成する手段と、
上記第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化する手段と、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して第２の証明用補助情報を生成する手段と、
上記暗号化した第１の証明用補助情報セットと上記第２の証明用補助情報セットとから複合的な証明用補助情報を生成して出力する手段とを有することを特徴とする証明用補助情報生成装置。
【請求項１１】　ユーザのアクセス資格を証明するために生成された証明データの正当性を検証することにより上記ユーザのアクセス資格を認証するアクセス資格認証装置に用いる証明用補助情報を生成する証明用補助情報生成方法において、

ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した第１の利用条件情報とに対し、所定の計算を実行して第１の証明用補助情報を生成するステップと、
上記第１の証明用補助情報と、上記第１の利用条件情報とからなる第１の証明用補助情報セットを暗号化するステップと、
上記ユーザの固有情報と、上記暗号化の復号鍵と、アクセス条件を記述した第２の利用条件情報とに対して、所定の計算を実行して第２の証明用補助情報を生成するステップとを有することを特徴とする証明用補助情報生成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザの権限を証明するために生成された証明データの正当性を検証することによりユーザのアクセス資格を認証する技術に関し、とくに上記証明データを生成する証明データ生成装置に関するものである。

【０００２】

【従来の技術】本発明と同分野に属する先行技術としてプログラムの実行制御技術が知られている。プログラム実行制御技術は、
①アプリケーションプログラム中にユーザ認証のためのルーチンを埋め込み、②該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
③前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合にはプログラムの実行を停止する技術である。

【０００３】このような技術を利用することにより、認証鍵を保有する正規のユーザにのみアプリケーションプログラムの実行を可能ならしめることが出来る。当技術はソフトウェア頒布事業において実用化されており、製品として、例えばＲａｉｎｂｏｗ Ｔｅｃｈｎｏｌｏｇｉｅｓ，Ｉｎｃ．社のＳｅｎｔｉｎｅｌＳｕｐｅｒＰｒｏ（商標）や、Ａｌａｄｄｉｎ Ｋｎｏｗｌｅｄｇｅ Ｓｙｓｔｅｍｓ Ｌｔｄ．社のＨＡＳＰ（商標）等がある。

【０００４】これらの技術では、ユーザの認証鍵は、ソフトウェアベンダが、複製を防ぐためにハードウェア中のメモリに厳重に封入し、郵便などの物理的手段を用いてユーザに配布し、ユーザはこれを所有のパソコンなどに装着して利用する。

【０００５】これらの技術は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならない。つまり、プログラム作成者は、鍵内蔵ハードウェアからの正しい返信をプログラム作成時に予測して、正しい返信を受けた場合にのみプログラムが正常に動作するようにプログラムの作成を行わなければならない。

【０００６】このような特徴を有する従来技術の利用形態は、基本的に以下の２通りとなる。

【０００７】①第１の方法では、ユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザ毎に異なる認証鍵を一つずつ用意する。

【０００８】②第２の方法では、プログラム作成者はアプリケーション毎にそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーション毎に異なる認証鍵を一つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。

【０００９】しかし、これらのいずれの場合にも、以下に述べるような問題を有する。

【００１０】第１の方法の場合、プログラム作成者は、プログラム中の認証ルーチンをユーザ毎に適切に変えてプログラムを作成する必要がある。つまり、ユーザ毎に認証鍵が異なるので、プログラム中の認証ルーチンは該プログラムを利用するユーザ固有の認証鍵を識別するように作成されなければならず、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。

【００１１】対象となるユーザが多数の場合、プログラムをユーザ毎に個別化する作業はプログラム作成者にとって耐えがたい労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。

【００１２】第２の方法の場合、第１の方法の場合のようにユーザ毎にプログラムを個別的に作成する必要は無くなるが、逆に、ユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないこととなる。

【００１３】この制約はプログラム作成者及びユーザそれぞれに以下のような問題を惹起する。

【００１４】前述のように、認証鍵はハードウェアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのと対照的に、認証鍵を内蔵するハードウェアの配布は郵便等の物理手段に頼らざるを得ない。この制限は、コスト、時間、梱包の手間いずれをとっても、プログラム作成者とって大きな負担となる。

【００１５】プログラム作成者は、ユーザの要求に応えるべく、アプリケーション毎に異なるハードウェアを一定個数ストックしておかなければならず、在庫管理のコストを必要とする。

【００１６】また、ユーザは利用するアプリケーションを変更する度にハードウェアを交換しなければならないという煩雑さに甘んじなければならない。

【００１７】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウェアが届くまで

待たねばならず、即座に利用できないという点での不便さも生ずる。

【００１８】この問題を解決する技術として、本出願人は新たなアクセス資格検証手法を提案している（特願平０８－０６２０７６号、現在未公開）。

【００１９】特願平０８－０６２０７６号の提案では、証明用補助情報（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させ、プロテクト側も、ユーザ側も１つの固有情報を準備しておけばすむようにしている。

【００２０】アクセスチケットは、特定のユーザの固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、また、ユーザ固有情報を知らずに、アクセスチケットからアクセス資格認証の特徴情報を計算することは困難である。そして、ユーザ固有情報とアクセスチケットとの正しい組み合わせ、すなわち、ユーザ固有情報と該ユーザ固有情報に基づいて計算されたアクセスチケットの組み合わせが入力された場合に限って、正しい証明用データが計算される。

【００２１】したがってユーザはあらかじめ固有情報を保持し、プログラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザのアクセス資格の認証を行う事ができる。

【００２２】この技術を用いて、アプリケーションプログラムにプロテクトを行ってユーザに配布し、アプリケーションプログラムの利用を希望するユーザに、アクセスチケットを提供するサービスが考えられる。

【００２３】希望するユーザに、ユーザ毎に異なる固有情報を封入したＩＣカードなどの媒体を渡しておき、またプログラム作成者はアクセス資格認証の特徴情報を用いてプログラムにプロテクトをかけて配布し、プログラムの利用を希望するユーザに、プログラム作成者またはプログラム作成者から委託を受けたチケット発行業者がアクセスチケットを提供する。

【００２４】このようなサービスを考えた場合、いつどのようにして課金するかということが問題になる。この例の場合では、アクセスチケットを発行する際に、チケットの発行と引換えにプログラムの代金に相当する料金を徴収することができる。

【００２５】ところで、このようなプログラムの利用権の売買サービスを考える場合、以下のような権利の形態が考えられる。

①パーチェス（ｐｕｒｃｈａｓｅ）：利用権を買いとってしまう方法。一度購入すると、永久に利用することができる。その後、利用する、しないにかかわらず、料金は同じである。

②ペイ・パー・ユース（ｐａｙ－ｐｅｒ－ｕｓｅ）：利用量課金とも呼ばれる。利用した量に応じて課金される。

③レント（ｒｅｎｔ）：一定期間の利用権を購入する。期限が過ぎれば利用できなくなる。

【００２６】前述の特願平０８－０６２０７６号の技術を用いた場合、パーチェスを実現することは容易であるが、レントを実現するのは困難である。

【００２７】ペイ・パー・ユースについては、利用する度毎にユーザが利用希望をチケット発行業者へ提出し、チケット発行業者は１回のみ使用可能なアクセスチケットを発行することにより実現することが可能であるが、頻繁にチケット発行操作が必要になる上に、１回のみ使用可能なアクセスチケットを実現するために、ユーザのＩＣカード中に使用したチケットに対するログを記録していく必要があるため、あまり現実的ではない。

【００２８】この問題に対しては、本出願人は利用制御情報をアクセスチケットの資格認証手法に導入することを提案している（特願平０８－１９１７５６号、現在未公開）。特願平０８－１９１７５６号の手法では、特願平０８－０６２０７６号に利用制御情報を導入し、情報を復号化する際に、この利用制御情報も用いるものである。利用制御情報の例としては、使用期限、使用可能回数、総使用可能時間、使用上限金額、処理の履歴を取るか否かの情報などが記載されている。

【００２９】利用制御情報が使用期限の場合には、レントを実現することが可能である。

【００３０】また利用制御情報が処理の履歴を取るという情報の場合には、一定期間後にその履歴を回収して集計することにより、利用した回数を計算し課金するという方法で、ペイ・パー・ユースに近い機能を実現することができる。さらに利用制御情報に１回あたりの利用額を記載するようにすれば、柔軟なペイ・パー・ユースを実現することが可能になる。

【００３１】つまり特願平０８－１９１７５６号の手法では、前述した権利の形態パーチェス、ペイ・パー・ユースおよびレントを全部実現できることになる。

【００３２】次に、支払の方法について考える。支払の方法としては、以下の２つが考えられる。

【００３３】①チケット発行時に支払う方法：チケット発行業者がアクセスチケットを発行する際に、支払う方法。電子貨幣により支払う場合や、発行業者側で料金を記録し、銀行振り込みなどにより清算を行う場合などがある。

【００３４】②プリペイドで支払う方法：ユーザが予めプリペイド度数を購入して、ＩＣカード中などに保持しておき、購入の際や利用の際に、プリペイドから相当する度数を引き落とす。

【００３５】特願平０８－１９１７５６号の技術を用いると、①チケット発行時に支払う方法で、前述した権利

の形態パーチェス、ペイ・パー・ユースおよびレントを全部実現できる。

【００３６】他方、②プリペイドで支払う方法では、ペイ・パー・ユースは容易に実現できる。つまり、利用制御情報に１回あたりの利用額を記載し、認証を行う度に、保持しているプリペイド情報から、利用制御情報記載の度数分ずつ引き落とせばよい。

【００３７】しかし、②プリペイドで支払う方法で、パーチェスやレントを実現するのは困難である。パーチェスは最初の利用時にのみプリペイドによる課金を行い、２回目以降の利用時には課金を行わないという処理が必要なためである。

【００３８】パーチェスに関しては、利用制御情報に利用権の買取り額を記載しておき、最初の利用時にその額を保持しているプリペイド情報から引き落として、該利用したアクセスチケットの情報をＩＣカードに登録するようにし、２回目以降の利用時には、利用しようとするチケットが既にＩＣカードに登録されているかをチェックして、登録されている時にはプリペイド情報から引き落とさないように構成することで実現することも可能ではある。しかし、この登録情報は、非常に長い期間消すことはできないので、多くのチケットを使うような場合には、ＩＣカードの記憶容量が不足することになり、あまり現実的な解決策ではない。

【００３９】レントの場合も、利用制御情報にレンタル額と有効期限を記載しておき、パーチェスと同様の方法を取ることで、実現することは可能ではあるが、同じくＩＣカードの記憶容量が不足することになり、あまり現実的な解決策ではない。

【００４０】

【発明が解決しようとする課題】本発明は、以上のような問題点に鑑みなされたものであり、プリペイドで支払う方法においても、証明データ生成装置（ＩＣカード）側に余分な負荷をかけることなく、パーチェスやレントを実現することを可能にすることを課題とする。

【００４１】

【課題を解決するための手段】本発明によれば、上述の課題を解決するために、ユーザのアクセス資格を認証するために生成され、正当性を検証される証明データを生成する証明データ生成装置に、認証用データを入力する認証用データ入力手段と、ユーザの固有情報を記憶するユーザ固有情報記憶手段と、ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス条件を記述した利用条件情報とに対し、所定の計算を実行して生成した証明用補助情報と、利用条件情報との組を含む証明用補助情報セットを記憶する証明用補助情報セット記憶手段と、入力された認証用データに対応する証明用補助情報セットを上記証明用補助情報セット記憶手段から取り出し、上記取り出した証明用補助情報セットの利用条件情報に従い、以降の処理を継続するかどうかの判断を行う利用条件判断手段と、上記利用条件判断手段において継続と判断されたときに、上記取り出した証明用補助情報セットと、上記認証用データ入力手段から入力された認証用データと、上記ユーザ固有情報記憶手段に記憶されている上記ユーザの固有情報とに所定の計算を施して証明データを生成し出力する証明データ生成出力手段とを設け、上記認証用データ入力手段から、第１の証明用補助情報セットを暗号関数における暗号化鍵で暗号化した暗号化証明用補助情報セットを入力し、上記利用条件判断手段は、上記証明用補助情報セット記憶手段から、入力された暗号化証明用補助情報セットに対応する第２の証明用補助情報セットを取り出し、上記取り出した第２の証明用補助情報セットの利用条件情報に従い、所定の処理を行った後、以降の処理を継続するかどうかの判断を行い、上記証明データ生成出力手段は、上記処理を行うことにより、上記暗号化証明用補助情報セットを復号化した結果である第１の証明用補助情報セットを出力するようにしている。

【００４２】つまり、通常の証明用補助情報セット（アクセスチケット）である第１の証明用補助情報セットを暗号化して暗号化証明用補助情報セットを作成しておき、この暗号化証明用補助情報セットへアクセスするための第２の証明用補助情報セットを用いて、通常の認証処理と全く同じ処理を行うことにより、暗号化証明用補助情報セットから、第１の証明用補助情報セットを復号化する。

【００４３】このように構成することにより、利用料金が無料のチケット（第１の証明用補助情報セット）を作成して暗号化し、暗号化されたチケットを復号化するためのチケット（第２の証明用補助情報セット）を発行し、このチケット（第２の証明用補助情報セット）の利用料金を有料としプリペイドで支払うように構成することで、全体としてプリペイドにおけるパーチェス機能の実現を可能にする。

【００４４】レント機能は、これに加えて第２の証明用補助情報セットの利用条件情報に有効期限情報を記載することで実現可能である。

【００４５】なお、暗号化されたチケットを復号化するには、通常のチケットの認証処理と同じ処理を行うように構成したので、比較的容量の少ないＩＣカード内に、余分なプログラムやデータを入れることなく、効率的に実現することが可能である。

【００４６】

【発明の実施の形態】以下、この発明の実施例について説明する。

【００４７】図１はこの実施例の構成図を示す。この実施例では、証明データ生成装置内にプリペイド情報を保持し、そのプリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する例（パーチェス）について説明する。

【００４８】図１では、証明データ生成装置で生成され出力された証明データを検証する証明データ検証装置を含めて示す。

【００４９】まず、図１に基づいて、本実施例の構成について説明したあと、証明データ検証装置、証明データ生成装置の処理の流れをフローチャートで示しながら説明する。処理の流れの説明には、通常の認証処理を例にして説明し、利用条件情報Ｌには、１回の利用の度ごとにプリペイドから引き落とされる例について説明する。そして、通常の認証処理の説明の後に、アプリケーションプログラムのアクセス権を購入する例（パーチェス）について説明する。

【００５０】［実施例の構成］図１は実施例の構成を全体として示すものであり、この図において、証明データ生成装置１０はユーザが保持するものであり、例えばＩＣカードのように内部に計算機能を持った携帯型の装置である。ＩＣカード以外にも、計算機能を持ったＰＣカードや、携帯型情報ツール、あるいはサブノートパソコンなどでもよい。内部の情報が、外部から簡単に改竄されたりすることがないように防御されていることが望ましい。

【００５１】証明データ検証装置２０はユーザがアプリケーションプログラムを使用するパソコンであり、パソコンのスロットに証明データ生成装置１０であるＩＣカードを装着して使用する。

【００５２】証明データ検証装置２０は、大きく認証用データ生成部２１と証明データ検証部２２とから構成されている。認証用データ生成部２１は、認証が必要な時に、認証用データを生成して、証明データ生成装置１０に送付する。証明データ検証部２２は、証明データ生成装置１０から送り返された証明データが正しいかどうかを検証する。

【００５３】アプリケーションプログラムは、暗号化などによりプロテクトされており、ユーザがアプリケーションプログラムを利用しようとすると、証明データ検証装置２０は、そのアプリケーションプログラムに対応した認証用データを作成し、証明データ生成装置１０に送り、証明データ生成装置１０から送り返された証明データを検証して、正しいと検証された場合に限り、アプリケーションプログラムのプロテクトを解除して、利用することを可能にする。

【００５４】一方、証明データ生成装置１０は、ユーザ固有情報記憶部１１、度数情報保持部１２、アクセスチケット記憶部１３、認証用データ入力部１４、利用条件判断部１５、証明データ生成出力部１６を含んで構成される。

【００５５】ユーザ固有情報記憶部１１は、ユーザの秘密情報を保持する部分であり、ユーザ毎に異なる情報である。ユーザ固有情報は、証明データ生成装置１０が作成された時に封入され、ユーザにも取り出せないように構成されていることが望ましい。

【００５６】度数情報保持部１２は、プリペイド情報を保持する部分であり、アプリケーションプログラムの利用や購入などに応じて、必要な額が減額されていく。額が少なくなった時には、増額することも可能である。増額の方法は、例えば、特願平９－２１３７３号で提案されている手法を用いることができる。この手法では、度数情報と署名した度数情報とを用いて度数情報を増額する。度数情報保持部１２における額の増減は、安全に行われることが必要であり、定められた方法以外でのアクセスができないように構成することが望ましい。

【００５７】アクセスチケット記憶部１３は、複数のアクセスチケットを記憶している。アクセスチケットは、ユーザにアクセス資格を与えるものであり、アプリケーションプログラム作成者、またはアプリケーションプログラム作成者から委託を受けたチケット発行業者によって作成される。本実施例では、アクセスチケットは、ユーザの固有情報と、アクセス資格認証の特徴情報と、アクセス資格認証のアクセス条件を記述した利用条件情報とに対し、所定の計算を実行して計算された証明用補助情報と利用条件情報との組である。本実施例では、アクセスチケット記憶部は、ＩＣカード中に構成されているが、アクセスチケットは発行された本人しか使えないため、コピーは自由であり、ＩＣカード外部に構成しても構わない。

【００５８】認証用データ入力部１４は、証明データ検証装置２０から送られた認証用データを入力する部分である。

【００５９】利用条件判断部１５は、入力された認証用データに対応するアクセスチケットをアクセスチケット記憶部１３から取り出し、アクセスチケット中の利用条件情報を元に、利用条件を判断する。例えば、アクセスチケットの有効期限が切れていないか、利用料金は保持しているプリペイドで支払うのに足りているか、などの利用条件を判断し、以降の処理を継続するか否かを判断する。

【００６０】証明データ生成出力部１６は、利用条件判断部１５で継続と判断された時のみ、証明データを生成して出力する。証明データは、利用条件判断部１５で取り出したアクセスチケット中の証明用補助情報と、認証用データと、ユーザの固有情報とに所定の計算を施して作成する。

【００６１】次に、具体例を挙げて、さらに詳細に説明する。ここでの説明は、通常の認証処理を例にして説明し、利用条件情報Ｌには、１回の利用の度ごとにプリペイドから引き落とされる例について説明する。

【００６２】図２は、図１の構成図に記号を付けたものである。記号は以下の説明と対応している。

【００６３】［通常の認証処理］以下では、法ｎにおけるＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｅｌｍａ

ｎ）暗号を用いた例について詳細に説明する。まず、通常の認証処理について説明する。以下の例では、アプリケーションプログラムの作成者であるソフトウェアベンダが、ＩＣカードの発行からチケットの発行まですべてを行う例について説明する。この例ではソフトウェアベンダは、すべてのユーザの秘密情報ｄｕを知っている。これ以外にも、ＩＣカードの発行とチケットとをチケット発行業者が行う構成も可能である。

【００６４】ソフトウェアベンダは、プロテクトしたいアプリケーションプログラムに対する暗号鍵を作成する。ここではＲＳＡ暗号を用いるので、大きな素数ｐ，ｑを秘密に作成し、法数ｎをｎ＝ｐ・ｑとして作成する。次に法数ｎの元で暗号鍵Ｅと復号鍵Ｄを、

【００６５】

【数１】$ED \equiv 1 \mod \phi(n)$

を満たすように生成する。ここでφ（ｎ）はオイラー数であり、φ（ｎ）＝（ｐ－１）（ｑ－１）である。

【００６６】次にソフトウェアベンダは、共通暗号鍵Ｋを作り、プロテクトしたいアプリケーションプログラムの一部または全部を、Ｋで暗号化し、

【００６７】

【数２】$K' = K^E \mod n$

を計算して、Ｋ’を暗号化したアプリケーションプログラムに、第３者が取り出せないように埋め込んで配布する。

【００６８】このアプリケーションプログラムを利用したいユーザは、予めこれに対応するアクセスチケットを入手しておくことになる。

【００６９】ソフトウェアベンダは、ユーザからのアクセスチケット発行要求を受けて、アクセスチケットを発行する。ソフトウェアベンダは、要求したユーザの秘密情報ｄｕと、アプリケーションプログラムの暗号化の際に用いた暗号鍵（Ｅ，ｎ）に対応する復号鍵（Ｄ，ｎ）とをデータベースから取り出す。次にアクセスチケットに付与する利用条件情報Ｌを作成する。ここではプリペイドから引き落として課金するので、１回の利用について引き落とす利用額をＬとする。そして、これらの情報を用いて、

【００７０】

【数３】$t = D - F(n, L, du)$

として証明用補助情報ｔを作成する。ここで関数Ｆ（）は一方向性の関数であり、一方向性ハッシュ関数ＭＤ５、ＳＨＡなどや、共通鍵暗号ＤＥＳ（ＤａｔａＥｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などを用いることができる。

【００７１】ソフトウェアベンダは、（ｔ，Ｌ，ｎ）の組をアクセスチケットとしてユーザに発行する。

【００７２】ユーザが、アプリケーションプログラムを利用しようとすると、証明データ検証装置は、そのアプリケーションプログラムに対応した認証用データ（Ｃ，ｎ）を作成し、証明データ生成装置に送る。

【００７３】この処理の流れを図３のフローチャートに示し、これに基づいて説明する。

（ステップＳ１１）：証明データ生成部２１は、プロテクトされたアプリケーションプログラムから、Ｋ’とｎとを取り出す。

（ステップＳ１２）：証明データ生成部は、乱数ｒを生成し、乱数保持部に格納する。

（ステップＳ１３）：$C = r^E K' \mod n$を計算する。

（ステップＳ１４）：（Ｃ，ｎ）の組を認証用データとして証明データ生成装置１０に送付する。

【００７４】次に、証明データ生成装置１０の流れを図４に示し、これに基づいて証明データ生成装置１０の処理を説明する。

（ステップＳ２１）：認証用データ入力部１４より、認証用データ（Ｃ，ｎ）を入力する。

（ステップＳ２２）：利用条件判断部１５は、ｎをキーにしてアクセスチケット記憶部を検索し、アクセスチケット（ｔ，Ｌ，ｎ）を取り出す。

（ステップＳ２３）：利用条件判断部１５は、取り出したアクセスチケット中の利用条件Ｌ（利用額）と、度数情報保持部の度数情報Ｖとを比較する。

（ステップＳ２４～Ｓ２５）：Ｖ≧Ｌの時は、証明データ生成出力部１６は、（ステップＳ２６）に進む。そうでないときは、証明データ生成出力部は、エラーを出力して終了する。

（ステップＳ２６）：利用条件判断部１５は、度数情報保持部１２に保持されている度数情報Ｖを利用条件（利用額）Ｌの分だけ減額する。

（ステップＳ２６～Ｓ２９）：証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報ｔ、利用条件Ｌ（利用額）と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算して出力する。

【００７５】

【数４】$R' = C^{F(n, L, du)} \mod n$

$R = C^t R' \mod n$

図４では、証明データＲを計算するのに、一旦Ｒ’の計算を分けている。これは、Ｒ’の計算にはユーザの秘密情報を用いるため、その処理が外部に漏れないように計算する必要があるが、一旦Ｒ’の計算が終われば、Ｒの計算は外部で行っても構わないためである。このようにＲ’とＲとに分けて計算してもよいし、一度に計算しても構わない。

【００７６】次に、証明データ検証装置２０の証明データ検証部の処理について説明する。証明データ生成装置１０から出力された証明データＲは、正しいユーザ固有情報ｄｕと、正しいアクセスチケット（正しい証明用補助情報ｔ、正しい利用条件Ｌ）を用いて計算されたとき

には、

【００７７】

【数５】

$$R = C^{t}R' \mod n$$
$$= C^{D-F(n,L,du)}C^{F(n,L,du)} \mod n$$
$$= C^{D} \mod n$$
$$= (r^{E}K')^{D} \mod n$$
$$= (r^{E}K^{E})^{D} \mod n$$
$$= (rK)^{ED} \mod n$$
$$= rK$$

となる。

【００７８】そこで、証明データ検証部２２では、乱数保持部２３から乱数ｒを取り出し、

【００７９】

【数６】 $r^{-1}R \mod n$

を計算することで、アプリケーションを暗号化していた共通暗号鍵Ｋを入手することができる。証明データ検証装置は、この共通暗号鍵Ｋでアプリケーションの暗号化されていた部分を復号し、アプリケーションを実行することができる。

【００８０】この例では、証明データ検証装置は、アプリケーションが正しく実行できたことをもって、正しく検証ができたと判断する。

【００８１】以上で通常の認証処理の説明を終了する。

【００８２】［パーチェス］次に、プリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する（パーチェス）例について説明する。

【００８３】この機能を実現するには、通常のアクセスチケットである第１のアクセスチケットを暗号化して暗号化アクセスチケットを作成しておき、この暗号化アクセスチケットへアクセスするための第２のアクセスチケットを用いて、通常の認証処理と全く同じ処理を行うことにより、暗号化アクセスチケットから、第１のアクセスチケットを復号化する。

【００８４】そしてこのとき、第１のアクセスチケットは、利用料金が無料のチケットとして作成し、第２のアクセスチケットは、利用料金を有料としプリペイドで支払うように構成することで、全体としてプリペイドにおけるパーチェス機能の実現を可能にする。

【００８５】まず、パーチェスの機能を実現したいアプリケーションプログラムをＡＰ１とする。上述の説明と同様に、ＡＰ１をプロテクトする。

【００８６】＜アプリケーションプログラムＡＰ１のプロテクトの説明＞ソフトウェアベンダは、プロテクトしたいアプリケーションプログラムに対する暗号鍵を作成する。ここではＲＳＡ暗号を用いるので、大きな素数p_1, q_1を秘密に作成し、法数n_1を$n_1 = p_1 \cdot q_1$として作成する。次に法数n_1の元で暗号鍵E_1と復号鍵D_1を、

【００８７】

【数７】 $E_1 \cdot D_1 \equiv 1 \mod \phi(n_1)$

を満たすように生成する。ここで$\phi(n_1)$はオイラー数であり、$\phi(n_1) = (p_1 - 1)(q_1 - 1)$である。

【００８８】次にソフトウェアベンダは、共通暗号鍵K_1を作り、プロテクトしたいアプリケーションプログラムの一部または全部をK_1で暗号化し、さらに共通暗号鍵K_1を以下の式に従って、暗号鍵E_1で暗号化して、K_1'を生成する。

【００８９】

【数８】 $K_1' = K_1E_1 \mod n_1$

そして、K_1'を暗号化したアプリケーションプログラムに、第３者が容易に取り出せないように埋め込んで配布する。また、n_1も、暗号化したアプリケーションプログラムに埋めこむ。

【００９０】ソフトウェアベンダは、作成した（n_1, D_1, $\phi(n_1)$）の組をアクセスチケット情報データベースに記憶する。

【００９１】次に、プリペイド払いパーチェス・チケットの作成について説明する。図５は、証明用補助情報生成装置３０の構成例を示したものである。この例では、第１の利用条件情報と第１の復号鍵とユーザ固有情報と第２の利用条件情報とを入力として、プリペイド払いパーチェス・チケットを出力する。図５において、入力部３１は、第１の利用条件情報と第１の復号鍵とユーザ固有情報と第２の利用条件情報とを入力する部分である。第１復号鍵記憶部３３は、入力部３１から入力された第１の復号鍵を記憶する部分である。第１の復号鍵は、アプリケーションプログラムＡＰ１の暗号化に用いた共通暗号鍵K_1を暗号化した暗号鍵（E_1, n_1）に対応する復号鍵（D_1, n_1）である。

【００９２】ユーザ固有情報記憶部３４は、入力部３１から入力されたユーザ固有情報を記憶する部分である。これは、ユーザの証明データ生成装置１０に格納されているものと同一のものである。

【００９３】ユーザがチケットの発行を依頼する時には、ユーザの識別情報Ｕと、ユーザが利用を希望するアプリケーションプログラムＡＰ１から取り出したn_1とを、ソフトウェアベンダに送る。ソフトウェアベンダは、ユーザの識別情報Ｕとユーザ固有情報ｄｕとを対応づけて保持しているユーザ情報データベースから、ユーザの識別情報Ｕに対応するユーザ固有情報ｄｕを検索することによってユーザ固有情報を得、また（ｎ，Ｄ，ϕ（ｎ））の組を保持しているアクセスチケット情報データベースから、n_1に対応する復号鍵（D_1, n_1）を得て、証明用補助情報生成装置３０に入力する。

【００９４】第１利用条件情報記憶部３２と第２利用条件情報記憶部３５は、それぞれ第１の利用条件情報と第２の利用条件情報とを記憶する部分である。第１の利用条件情報は、アプリケーションプログラムＡＰ１の利用

条件を記述したものであり、第２の利用条件情報は、プリペイド払いパーチェス・チケットの利用条件を記述したものである。プリペイド払いパーチェス・チケットの場合には、１回目の利用時に課金され、２回目以降の利用時には課金されないという特性を持つので、第１の利用条件情報には少なくとも無料であることを意味する情報が含まれており、第２の利用条件情報には、少なくとも有料であることを意味する情報が含まれている。

【００９５】第１チケット生成部３６は、入力された第１の利用条件情報と第１の復号鍵とユーザ固有情報とに所定の計算を実行してアクセスチケットを生成する部分である。

【００９６】第１利用条件情報記憶部３２と第１復号鍵記憶部３３とユーザ固有情報記憶部３４と第１チケット生成部３６とからなる構成部分４１は、通常のアクセスチケットを生成するのと同様の構成をなしている。

【００９７】第２の鍵生成部３７は、第１チケット生成部３６で生成された第１のアクセスチケットを暗号化するための鍵を生成する部分である。

【００９８】暗号化部３８は、第１チケット生成部３６で生成された第１のアクセスチケットを、第２の鍵生成部３７で生成された暗号化鍵を用いて暗号化する部分である。

【００９９】第２チケット生成部３９は、暗号化部３８で暗号化された暗号化アクセスチケットを復号化するために必要となる第２のアクセスチケットを生成する部分である。

【０１００】チケット出力部４０は、暗号化部３８で暗号化された暗号化アクセスチケットと、第２チケット生成部３９で生成された第２のアクセスチケットとを組み合わせて、プリペイド払いパーチェス・チケットとして出力する。

【０１０１】＜プリペイド払いパーチェス・チケットの作成＞以下に、プリペイド払いパーチェス・チケットの作成の方法について図６のフローチャートを用いて説明する。

【０１０２】ソフトウェアベンダは、ユーザからのプリペイド払いパーチェス・チケット発行要求を受けて、プリペイド払いパーチェス・チケットを発行する。チケットの発行を依頼するユーザは、ユーザの識別情報Ｕと、ユーザが利用を希望するアプリケーションプログラムＡＰ１から取り出したn_1とを、ソフトウェアベンダに送る。

【０１０３】（ステップＳ３１）：ソフトウェアベンダは、ユーザからのプリペイド払いパーチェス・チケット発行要求であるユーザの識別情報Ｕとアプリケーションプログラムａｐ１から取り出したn_1との組（Ｕ，n_1）を入力する。また、アプリケーションプログラムＡＰ１の利用条件を記述した第１の利用条件情報L_1と、プリペイド払いパーチェス・チケットの利用条件を記述した第２の利用条件情報L_2も入力する。ここでは、プリペイド払いパーチェス・チケットの生成を目的としているので、第１の利用条件情報L_1は、利用料金が無料であることを意味する

【０１０４】

【数９】$L_1=0$

であり、第２の利用条件情報Ｌ２は、パーチェスの料金が有料であることを意味する

【０１０５】

【数１０】$L_2=A$

とする。ただしＡは０以外の数字であり、たとえば１００である。

【０１０６】（ステップＳ３２）：ユーザの識別情報Ｕとユーザ固有情報ｄｕとを対応づけて保持しているユーザ情報データベースから、ユーザの識別情報Ｕに対応するユーザ固有情報ｄｕを検索する。

（ステップＳ３３）：（ｎ，Ｄ，ϕ（ｎ））の組を保持しているアクセスチケット情報データベースから、n_1に対応する第１の復号鍵（D_1，n_1）を検索する。

（ステップＳ３４）：ユーザがＡＰ１にアクセスするための第１のアクセスチケットT_1を作成する。

【０１０７】

【数１１】$T_1=(t_1, L_1, n_1)$

$t_1=D_1-F(n_1, L_1, du)$

（ステップＳ３５）：第１のアクセスチケットT_1を暗号化するために、第２の法数n_2、第２の暗号鍵E_2、第２の復号鍵D_2を生成する。大きな素数p_2，q_2を生成し、以下の式が成り立つように、法数n_2、暗号鍵E_2、復号鍵D_2を生成する。

【０１０８】

【数１２】$n_2=p_2\cdot q_2$

$E_2\cdot D_2\equiv 1 \mod \phi(n_2)$

$\phi(n_2)=(p_2-1)(q_2-1)$

（ステップＳ３６）：生成した第２の暗号鍵E_2で第１のアクセスチケットT_1を暗号化する。T_1を暗号化したものをT_1'とする。

【０１０９】

【数１３】$T_1'=T_1E_2 \mod n_2$

（ステップＳ３７）：暗号化されたアクセスチケットT_1'をユーザが復号するための第２のアクセスチケットT_2を作成する。

【０１１０】

【数１４】$T_2=(t_2, L_2, n_2)$

$t_2=D_2-F(n_2, L_2, du)$

（ステップＳ３８）：（（T_1'，n_2），T_2）を組にしてプリペイド払いパーチェス・チケットとして出力する。

【０１１１】ソフトウェアベンダは、出力されたプリペイド払いパーチェス・チケット（（T_1'，n_2），T_2）を、ユーザに送付する。

【０１１２】次に、プリペイド払いパーチェス・チケットの使用例について説明する。

【０１１３】＜プリペイド払いパーチェス・チケットの使用例＞

（ａ）プリペイド払いパーチェス・チケット（（T_1'，n_2），T_2）を受け取ったユーザは、まずT_2をアクセスチケット記憶部１３に格納する。

（ｂ）次に、（T_1'，n_2）を自分が保持している証明データ生成装置１０の認証用データ入力部１４より入力する。

【０１１４】以下、証明データ生成装置１０における処理が図４に従って行われる。今、証明データ生成装置１４の度数情報保持部１２には、８００度数のプリペイド情報Ｖが保持されているとする。（Ｖ＝８００）

（ステップＳ２１）：認証用データ入力部１４より、認証用データ（T_1'，n_2）を入力する。

（ステップＳ２２）：利用条件判断部１５は、n_2をキーにしてアクセスチケット記憶部１３を検索し、アクセスチケットT_2＝（t_2，L_2，n_2）を取り出す。

（ステップＳ２３）：利用条件判断部１５は、取り出したアクセスチケット中の利用条件L_2と、度数情報保持部１２の度数情報Ｖとを比較する。

（ステップＳ２４）：今、L_2＝１００、Ｖ＝８００なので、

【０１１５】

【数１５】$V \geqq L_2$

が成り立ち、（ステップＳ２６）へ進む。

（ステップＳ２６）：利用条件判断部１５は、度数情報保持部１２に保持されている度数情報Ｖを利用条件L_2の分だけ減額する。

【０１１６】

【数１６】Ｖ＝８００－１００＝７００

つまり、度数情報Ｖは、プリペイド払いパーチェス・チケットの買取り料金として、１００度数引き落とされ、残り７００度数となる。

（ステップＳ２７～Ｓ２９）：証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報t_2、利用条件L_2と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算して出力する。

【０１１７】

【数１７】$R' = T_1'^{F(n2, L2, du)} \mod n_2$

$R = T_1'^{t2} R' \mod n_2$

Ｒの計算を行うと、

【０１１８】

【数１８】

$R = T_1'^{t2} R' \mod n_2$

$= T_1'^{D2-F(n2, L2, du)} C^{F(n2, L2, du)} \mod n_2$

$= T_1'^{D2} \mod n_2$

$= (T_1^{E2})^{D2} \mod n_2$

$= T_1$

という計算が成り立ち、証明データ生成出力部１６から、証明データＲとして

【０１１９】

【数１９】$R = T_1$

が出力される。

【０１２０】つまり、（T_1'，n_2）を自分が保持している証明データ生成装置１０の認証用データ入力部１４より入力すると、L_2が度数情報Ｖから引き落とされて、結果としてT_1'が復号されたT_1が出力される。

【０１２１】（ｃ）ユーザは、入手したT_1をアクセスチケット記憶部１３に格納する。

【０１２２】（ｄ）ユーザは、アプリケーションプログラムＡＰ１を利用するためのアクセスチケットT_1を入手できたので、アプリケーションプログラムＡＰ１を利用する。

【０１２３】以下、証明データ検証装置１０における認証用データ生成処理が図３に従って行われる。

（ステップＳ１１）：認証用データ生成部２１は、プロテクトされたアプリケーションプログラムから、K_1'とn_1とを取り出す。

（ステップＳ１２）：認証用データ生成部２１は、乱数ｒを生成し、乱数保持部２３に格納する。

（ステップＳ１３）：$C = r^E K_1' \mod n_1$を計算する。

（ステップＳ１４）：（Ｃ，n_1）の組を認証用データとして証明データ生成装置１０に送付する。

（ｅ）証明データ生成装置１０における処理が再び図４に従って行われる。

（ステップＳ２１）：認証用データ入力部１４より、認証用データ（Ｃ，n_1）を入力する。

（ステップＳ２２）：利用条件判断部１５は、n_1をキーにしてアクセスチケット記憶部１３を検索し、アクセスチケットT_1＝（t_1，L_1，n_1）を取り出す。

（ステップＳ２３）：利用条件判断部１５は、取り出したアクセスチケット中の利用条件L_1と、度数情報保持部１２の度数情報Ｖとを比較する。

（ステップＳ２４）：今、Ｌ１＝０、Ｖ＝７００なので、

【０１２４】

【数２０】$V \geqq L_1$

が成り立ち、（ステップＳ２６）へ進む。

（ステップＳ２６）：利用条件判断部１５は、度数情報保持部１２に保持されている度数情報Ｖを利用条件L_1の分だけ減額する。

【０１２５】

【数２１】Ｖ＝７００－０＝７００

つまり、度数情報Ｖは、最初にプリペイド払いパーチェス・チケットの買取り料金として、１００度数引き落とされているので、２回目以降の利用では引き落とされ

ず、残り７００度数のままとなる。

（ステップＳ２７～Ｓ２９）：証明データ生成出力部１６は、利用条件判断部１５が取り出した証明用補助情報t_1、利用条件L_1と、ユーザ固有情報記憶部１１から読み出したｄｕとを用いて証明データＲを計算して出力する。

【０１２６】

【数２２】$R' = C^{F(n1, L1, du)} \mod n_1$

$R = C^{u}R' \mod n_1$

つまり、

【０１２７】

【数２３】

$R = C^{u}R' \mod n_1$

$= r^{K}$

（ｆ）証明データ検証装置２０の証明データ検証部２２は通常の認証と同様に処理を行い、乱数保持部２３から乱数ｒを取り出し、

【０１２８】

【数２４】$r^{-1}R \mod n_1$

を計算することで、アプリケーションを暗号化していた共通暗号鍵Ｋを入手することができる。証明データ検証装置は、この共通暗号鍵Ｋでアプリケーションの暗号化されていた部分を復号し、アプリケーションを実行することができる。

【０１２９】これ以降は、何度アプリケーションプログラムＡＰ１を実行しても、同様の処理が行われ、無料で利用することができる。

【０１３０】以上説明したように、上記のように構成することで、プリペイド情報を用いて、アプリケーションプログラムのアクセス権を購入する（パーチェス）ことが可能になる。

【０１３１】以上、プリペイドにおけるパーチェス機能の実現について説明した。

【０１３２】これ以外にも、証明データ生成装置に時計を備え、第１のアクセスチケットの利用条件情報Ｌの中に、利用額が無料という情報に加えて、有効期限情報を記載し、第１のアクセスチケットの利用のたびに、時刻と比較することによって、プリペイドにおけるレント機能を実現することも可能である。

【０１３３】さらに、別の例としては、証明データ生成装置に時計を備え、第２のアクセスチケットの利用条件情報Ｌの中に、有効期限情報を記載し、暗号化された第１のアクセスチケットの復号の際に、時刻と比較することによって、第１のアクセスチケットを配布（解凍）する期限を限定することなども可能である。

【０１３４】また、本実施例では、ＲＳＡ暗号を元にして説明を行ったが、これに限らず他の暗号方式を用いても構わない。また、アクセスチケットの実現式もこれに限ることはない。

【０１３５】

【発明の効果】実行制御等のユーザのアクセス資格の認証を行うに際して、ユーザはあらかじめ固有情報を保持し、プログラム作成者等のプロテクト者はユーザが所持する固有情報とは独立にアクセス資格認証の特徴情報を用意し、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセス資格認証の特徴情報とに応じて作成し、配布することにより、ユーザおよびプロテクト者の双方を、アクセス権情報管理のわずらわしさから開放させるという特徴を残したまま、従来は困難だったプリペイドにおけるパーチェス機能およびレント機能を実現することを可能にした。

【０１３６】さらにこれらの機能を実現するにおいて、通常のチケットの認証処理と同じ処理を行うように構成したので、比較的容量の少ないＩＣカード内に、余分なプログラムやデータを入れることなく、効率的に実現することが可能である。

【図面の簡単な説明】

【図１】　本発明の実施例の構成を示すブロック図である。

【図２】　図１の構成を詳細に説明する図である。

【図３】　図１の証明データ検証装置の認証用データ生成処理を説明するフローチャートである。

【図４】　図１の証明データ生成装置の証明データ生成処理を説明するフローチャートである。

【図５】　図１の証明データの生成に用いるチケットを生成する証明用補助情報生成装置を示すブロック図である。

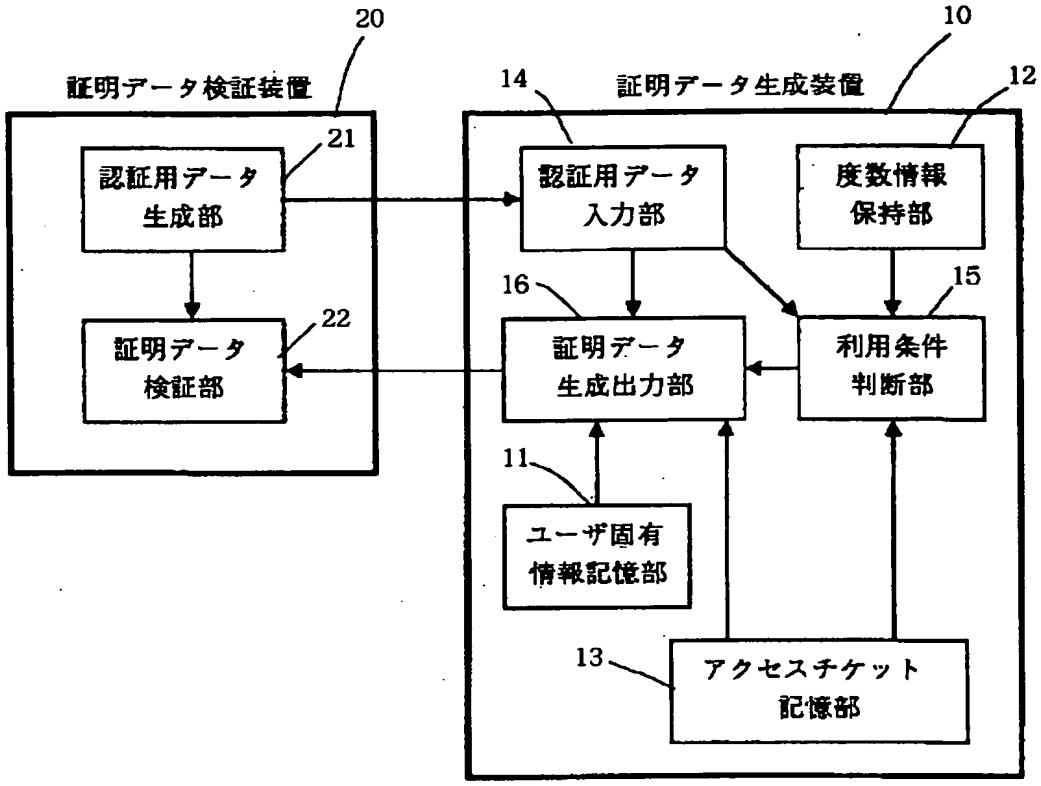
【図６】　図１の証明データの生成に用いるチケットの生成を説明する図である。

【符号の説明】

１０　証明データ生成装置
１１　ユーザ固有情報記憶部
１２　度数情報保持部
１３　アクセスチケット記憶部
１４　認証用データ入力部
１５　利用条件判断部
１６　証明データ生成出力部
２０　証明データ検証装置
２１　認証用データ生成部
２２　証明データ検証部
２３　乱数保持部
３０　証明用補助情報生成装置
３２　第１利用条件情報記憶部
３３　第１復号鍵記憶部
３４　ユーザ固有情報記憶部
３５　第２利用条件記憶部
３６　第１チケット生成部
３７　第２の鍵生成部
３８　暗号化部
３９　第２チケット生成部

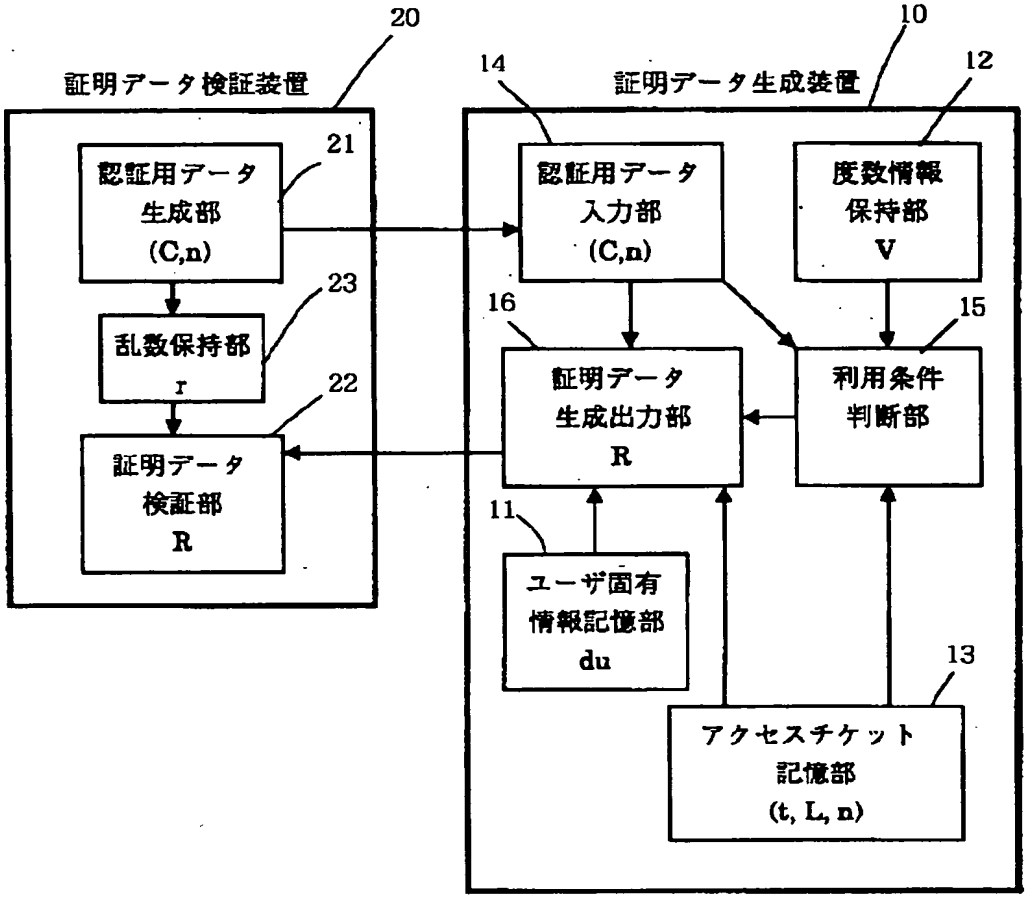
４０　チケット出力部

【図１】



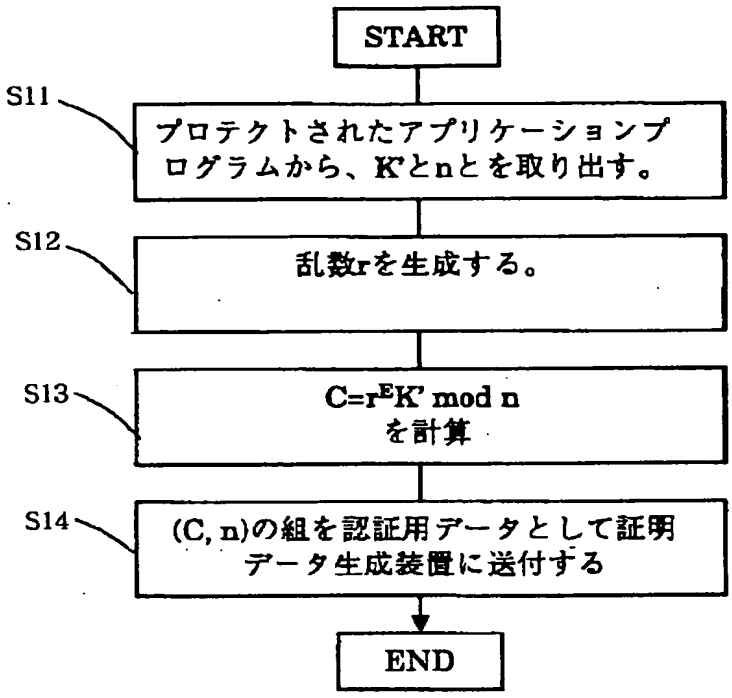
実施例の構成図

【図２】



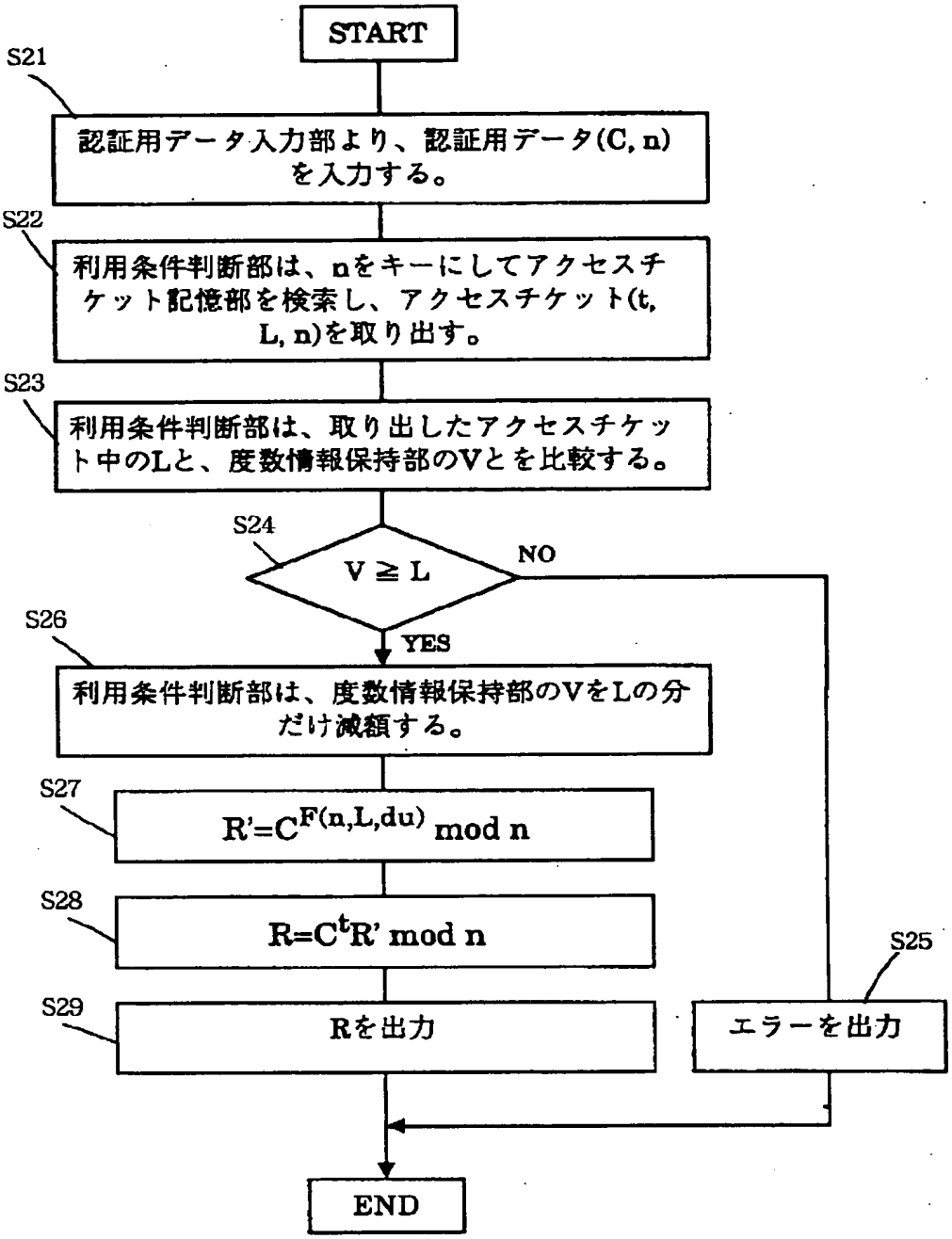
実施例の詳細構成図

【図３】



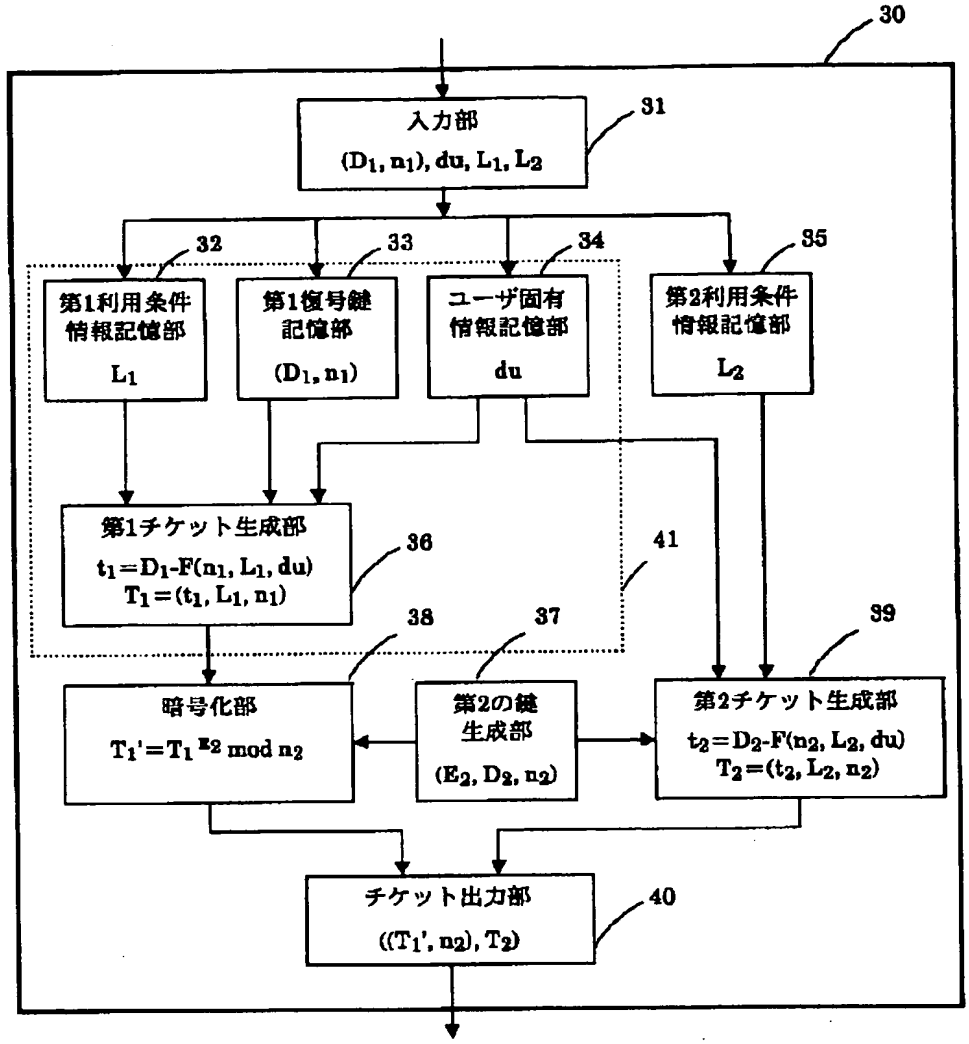
証明データ検証装置における認証用データ生成処理

【図４】



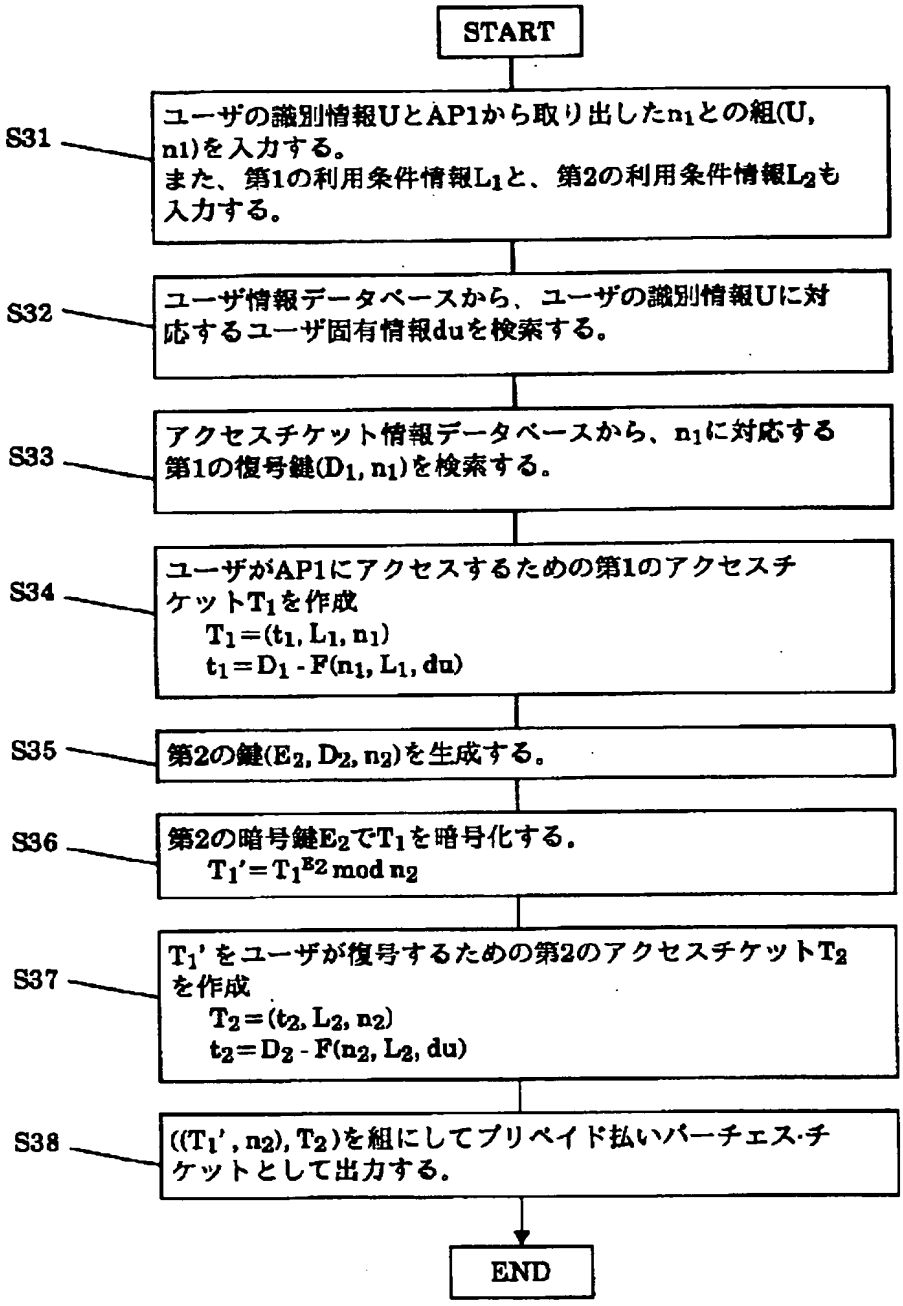
証明データ生成装置における処理

【図５】



証明用補助情報生成装置の構成図

【図６】



プリペイド払いパーチェスチケット作成処理